February 2016

Volume 1, Issue 5

SITSD
Enterprise Security
Program

Security Matters

Focus on Identity Theft

When we think of hackers we often think about people who want to clean out our bank accounts and run up a huge bill on our credit cards. While that's a serious matter, the more difficult situation in which to find yourself is that of having your identity stolen.

Identity theft is when another person uses you Social Security number and/or other personal information to open accounts, get credit, make purchases, get tax refunds. In short, the criminal is looking for a long-term economic gain, not just the quick theft of the contents of your bank account. In some cases the thief goes further and poses as the victim to buy guns, get loans for homes and cars, or even file for bankruptcy to attempt to destroy the victim's credit and life. In the last few years, the theft of personal health information has also led to cases where the criminal uses the victim's identity to obtain medical care and prescription drugs.

While having your credit card information stolen is disruptive, there are legal limits to your liability if that happens. It can take thousands of dollars and years to recover from identity theft.

Criminals may obtain personal data by both physical and digital methods. Pre-approved credit card applications can be retrieved from the trash and used to activate the cards. If you use your mobile device in public areas, thieves may listen as you provide a credit card number to someone like a hotel reservations clerk. They may "shoulder surf" as you shop or bank online to get your credit card number or other information.

Mailboxes also are a source of information. Most of us receive bills, bank statements, credit cards, boxes of checks, and other official documents through the mail. These can be easily stolen from an unlocked mailbox.

Continued on page 5

February 9th is Safer Internet Day (SID). SID was started in Europe in 2004 to raise awareness of online issues and has now become a global celebration. Each year there are events and activities to promote safer and more responsible use of online technology and mobile phones, especially among children and young people. In 2016 the focus is "Play your part for a better internet".

Learn how each of us can contribute to creating a better online environment by visiting the SID website , registering as a supporter, and downloading resources to promote the message of a safer, better internet.

https://www.saferinternetday.org

Security Matters is the monthly information security newsletter published by the Enterprise Security Program. Each month we also have a supplemental file of materials you can use for security awareness. You can find that file at: http://sitsd.mt.gov/Montana-Information-Security/Security-Training-Resources

We hope you'll find the newsletter and materials useful and hope you'll give us feedback on what we can do better. Your suggestions for topics and content are welcome. Contact us.

Inside this issue:

A monthly update on the latest security threats and other software news.

TAX IDENTITY THEFT PREVENTION TIPS

Last month we gave you some tips about preventing tax fraud. With tax season getting into full swing and Tax Identity Theft Awareness Week at the end of January we thought we'd revisit the topic and share some tips from the Federal Trade Commission. (If you follow our Facebook page Montana Information Security you've already seen these.)

Tax identity theft happens when someone files a fake tax return using your personal information — like your Social Security number — to get a tax refund or a job. The best thing to do is file early in the tax season — if you can — to get your refund before identity thieves do. When you file, make sure you use a secure internet connection or mail your tax return directly from the post office to make it more difficult for thieves to get their hands on your personal information.

What should you do if you think your Social Security number has been stolen? Or if you get a letter from the IRS saying more than one tax return was filed in your name, or that IRS records show wages from an employer you don't know? Call the IRS Identity Theft Protection Specialized Unit at 1-800-908-4490. If you are a tax identity theft victim, the IRS may give you a personal PIN number to verify your identity and protect your file going forward.

Have you heard about IRS imposters? Tax scammers posing as the IRS call and say you owe taxes, and threaten to arrest you if you don't pay with a prepaid debit cards or credit card. They might know some information about you, and they can rig caller ID to make it look like the IRS is calling. But the IRS won't ask you to pay with prepaid debit cards or wire transfers, and won't ask for a credit card number over the phone. If the IRS needs to contact you, they will first do it by mail. If you have any doubts, call the IRS directly.

Here are some tips to reduce the risk of being a victim of tax identity theft:

- Always protect your Social Security number or Medicare card number: don't give it out unless you have to, and always ask why it's needed, how it's going to be used, and how it will be stored.
- Shred old taxes returns you're no longer required to keep, as well as draft returns, extra copies, and calculation sheets.
- Ask for recommendations and research tax preparers before you turn your personal information over to them.

Once tax identity thieves have your Social Security number and personal information, they can use them to commit other forms of identity theft, such as opening new financial accounts in your name.

Go to IdentityTheft.gov to report identity theft, get step-by-step advice, sample letters, and your FTC Identity Theft Affidavit. These resources will help you fix problems caused by the theft.

Security Awareness 2016 Events

Focus on Identity Theft

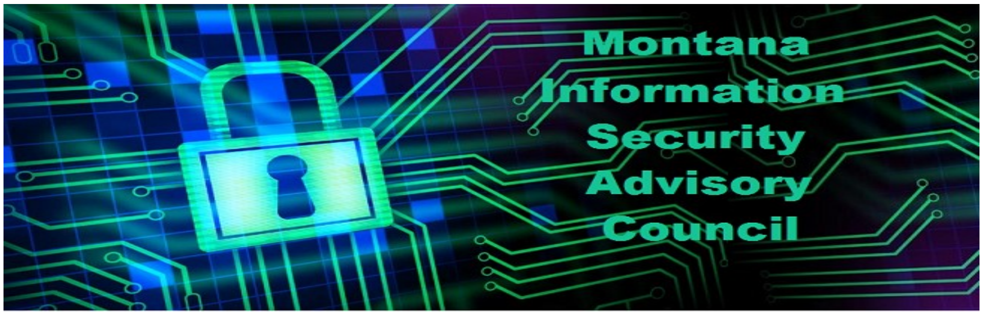
- Feb 9, 2016 - 10:30—1:30 at DOC Conference Room 228
  301 S Park Ave.

Focus on Cyber Espionage

Focus on Email

- April 14, 2016 - 1:30—3:30 at OPI Training Room
  1227 11th Ave

We do not have a March event scheduled yet. Please contact Lisa Vasa if you'd like to host an event in March—or any other month—at your location. The focus topic is cyber espionage. We do all the work as well as provide treats, giveaways, and prizes. All you need to do is schedule a room and do a little bit of promotion (and we help with that, too). We make it easy and fun for you to bring security awareness training to your agency!



Meeting Highlights of the Montana Information Security Advisory Council Meeting & Preview of the Upcoming Meeting

January 20, 2016 Meeting highlights

Data Classification Policy

Lynne Pizzini discussed the Data Classification Policy and Guideline changes. These changes were discussed at the January 6th ITMC meeting and have been posted to the ITMC website for review. The changes will be discussed and voted on during the February 3rd ITMC meeting.

Guest Speaker

Ben Spear from Multi State – Information Sharing and Analysis Center (MS-ISAC) discussed common cyber threats affecting state, local, tribal, and territorial governments. His detailed discussion included malware issue differences between 2014 and 2015. To aid in cyber threats and loss of information, Spear suggested agencies ensure they have adequate backups of all information in case they need to recover information. The Cryptowall ransomware remains the highest malware issue of 2015. To help with issues of website defacement, agencies should ensure all plugins are up to date. Patching systems with latest security patches continues to be best defense against threats. Issues that are increasing in 2016 include media reporting, university targeting, extortion-based activity, complex attack vectors, big data, internet infrastructure changes, gubernatorial initiatives, and patching.

MT-ISAC now has a SharePoint site for collaboration for the workgroups and there was a demo of the SharePoint site. All Council approved documents from the workgroups will be posted to the MT-ISAC website for all to see. Work in progress and ideas for future efforts will be stored on the SharePoint site. Currently only state users can access the SharePoint site.

Approved Objectives

There are a total of 37 objectives listed from the MT-ISAC Goals and Objectives document. Five were approved as accomplished by the Council. Those objectives that were approved were as follows:

* Implement a comprehensive information security awareness and training program.
* Help as a resource, security and awareness training and professional security training for managers, users, contracted support, and IT staff.
* Develop a campaign to deliver the message of information security in a positive and informational manner that engages the listener and encourages them to integrate information security into their daily activities.
* Update State of Montana information security policies and documents to align with the NIST Cybersecurity Framework.
* Share risk management guidance and recommendations with local governments and the private sector.

Assessment Workgroup

The Assessment workgroup demoed the assessment document that is currently be worked on. This document will be a reference for agencies to use to measure their agency's compliance with the Information Security Policy. This is a self-assessment document for each agency.

Best Practices Workgroup

The Best Practices workgroup discussed a "Device Hardening Strategy" document. This document is on the MT-ISAC website for review and comments.

Situational Awareness Workgroup

The Situational Awareness workgroup reported that the group is drafting an incident response report for high level incidents.

2015 Incident Report

Sean Rivera reviewed the incident reports for the State of Montana for calendar year 2015. The warning and critical incidents are reported from the SITSD service desk to State agencies, cities, and counties. More threats were blocked in 2015 than any prior year.

Next Meeting

The next meeting will be **Thursday,** February 18, 2016 at 1:00 p.m. at the DEQ Lee Metcalf Building, Room 111. **Please note that the meeting has changed from the third Wednesday of the month to the third Thursday.**

NEW MT-ISAC SharePoint Site

The Montana Information Security Advisory Council now has a MT-ISAC SharePoint site. This SharePoint site is only available to those who have state active directory credentials at this time. The MT-ISAC website will still be where agendas to meetings and approved documents will be stored. For more information contact the Enterprise Security Program.

Security Training News

DHS Training Grant Recipients

A panel of MT-ISAC members have awarded professional security training classes to seven individuals. Classes will be purchased using a grant from the Department of Homeland Security (DHS). Congratulations to the following people:

Mike Manzanec—Montana University System

John Cross—Dept Labor & Industry

Curt Norman—Office of Public Instruction

Erika Billiet—City of Kalispell

Jason Emery—City of Missoula

Chris Sinrud—City of Helena

Tim Kosena—Montana Supreme Court

Twenty people applied for the grant-funded classes. The Enterprise Security Program (ESP) will be applying for additional grant funding later this year, also to be used to provide security training to Montana state, local, and tribal government employees.

January Prize Winners FWP Security Awareness Event

Auto Emergency Kit	Shari Risken
Dairy Queen Gift Card	Linnaea Schroeer
Cinemax Movie Gift Card	Kari Shinn
Amazon Gift Card	Dee Burnham
Starbucks Gift Card	Xander Kennedy

FREE Security Professional Training

Dawn Temple at DOJ gave us a heads up about this month's FREE professional training resource: Texas A&M Engineering Extension Service (TEEX). Not all of it is for technical users—there are three tracks each focused on one of the following disciplines: general, non-technical computer users; technical IT professionals; and business managers and professionals. You can check out TEEX at: https://teex.org/Pages/Program.aspx?catID=607&courseTitle=Cybersecurity#.

Security Engineering—Applied Cyber Security

OpenLearning is a free learning community bringing together students and institutions from all over the word. Beginning February 28, 2016 they will be releasing a series of courses in cyber security. For more information see https://www.openlearning.com/courses/sec.

Dizzy New World of Cyber Investigations: Law, Ethics, and Evidence

Virtual Event—February 18, 2016 11:00 AM MST

Increasingly, employers and enterprises are engaged in cyber investigations. The explosion of cyber evidence (email text, metadata, social media, big data, etc.) about every little thing that anyone does or says creates a massive need for HR departments, IT departments, internal audit departments and other investigators to find and sift through this evidence. These cyber investigations are guided, motivated, and restricted by a blizzard of new laws and court cases. Increasingly enterprises need professionals with background in cyber forensics, cyber law, and computer privacy . Registration

Federal Virtual Training Environment (FedVTE)

We want to remind you about the FedVTE cybersecurity training system. Courses range from beginner to advanced levels and are available at no cost to users. Sign up is easy at: www.Fedvte.usalearning.gov and a catalog of available courses is on the site. Also, look for announcements regularly for opportunities to participate in the FedVTE Live! Classes. These classes use an interactive virtual live classroom and are the next best thing to being there. Space is limited so respond quickly to announcements if you are interested.

For more security training and awareness resources, check out the Security Training Resources page and watch for more information here each month.

Focus continued from page 1

Phishing emails are another way criminals get personal information from potential victims. These emails attempt to trick the recipient into providing user IDs, passwords, account numbers, and other details.

Social media is great for staying in touch but it's also a wealth personal information. Users often share details which seem harmless, but when put together can provide enough information to help a determined identity thief. Birthdays, family relationships, workplaces, children's and pet's names all may provide clues to passwords as well as background information that may be used to obtain account access.

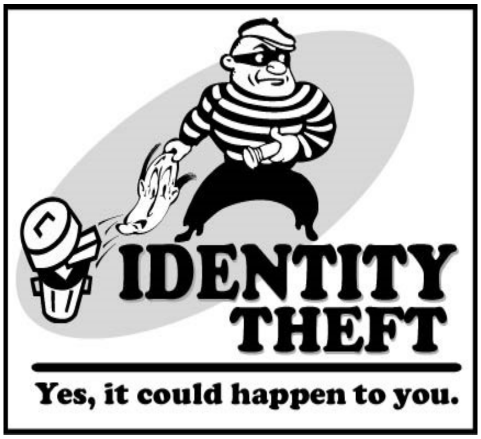
Outside of our personal control are data breaches, but they, too, may provide information to identity thieves. It seems like more and more we are learning of breaches at retailers, health providers, insurance companies, and even the government.

Avoiding Identity Theft

Start by using care with the information you share. Only provide personal information to people and companies that have a legitimate need for the information.

When using social media, use your privacy settings to restrict access to your personal information. Don't base your passwords on information about you that is shared publicly like children's and pet's names, birthdays, etc.

If you receive an email or phone call from someone who offers you prizes or a special loan or credit card offer but requires that you provide personal information to take advantage of the offer, ask them to send you a written form and, if they do, verify that it will be submitted to a reputable company.



Be suspicious of threatening emails or phone calls that ask for account information, passwords, Social Security numbers, etc. Your bank or credit card company may ask for the last four digits of your Social Security or account number, but they already have the full number on file and should only be using the last digits to verify information they already have.

When using mobile devices in public make sure that your device can't be seen by others. If you need to provide personal information over the phone to someone, do it in a private location so others can't listen to your call.

Pay attention to bills and bank statements that are mailed to you. If you don't receive them as expected, call the company or financial institution to make sure they are being sent to the correct location. Consider using a locking mail box or a box at the local Post Office to provide additional protection.

Review your monthly statements carefully to check for unauthorized charges. If your bank or credit card company provides activity alerts, sign up to receive them. If you see unauthorized transactions, contact the financial institution immediately. Also read your health insurance statements to verify any claims.

Check your credit report regularly. You can request a copy free of charge once per year from each credit reporting agency (Experian, Equifax, and TransUnion). You may also want to sign up for a credit monitoring service which allows you to check your reports at any time and can send alerts based on activity such as a new inquiry or accounts.

Use care when disposing of documents with personal information, including the aforementioned credit card offers. Consider buying and using a shredder that will shred credit cards as well as paper.

Signs of Identity Theft

Despite doing your best to avoid being a victim of identity theft, it is still possible that someone will find a way to steal your identity. Be on the lookout for charges you didn't make on your credit cards or withdrawals from financial accounts. You may receive overdraft notices or calls from debt collectors about accounts that are not yours. You may have health insurance claims rejected due to reaching your benefit limits or conditions that you don't have may show up on your medical records. Identity thieves may file tax returns in your name causing the IRS to notify you of duplicate returns.

Respond to Identity Theft

If you think you have been a victim of identity theft, take steps quickly to limit the damage.

- Call the companies or financial institutions where unauthorized activity occurred to report the fraudulent transactions.
- Place a fraud alert with credit reporting companies and request copies of your credit report.
- File a report with local law enforcement.
- Visit the Federal Trade Commission's (FTC) Identity Theft website https://www.identitytheft.gov to file a report, find resources, and make a plan for recovering from identity theft.

Identity theft is a serious issue. Protecting your personal information, sharing with care, and being suspicious of unusual requests for your information can help prevent identity theft. Knowing your rights and how to respond if you are a victim will help you recover. Remember, there's only one of you!

News You Can Use

Identity theft complaints leap 47%

According to the Federal Trade Commission, reports of identity theft were up 47% in 2015, driven by an increase in tax and wage-related fraud.

How your kid could become a victim of identity theft

If you don't have enough to worry about when raising kids, add identity theft to the list.

User education is the first line of defense against ransomware

"There are numerous strategies for safeguarding against ransomware. The first, and by far the most effective, is user awareness and education, because ransomware does not install itself."

YOU'RE REPLYING TO A TAX PHISHING SCAM?
SECURITY CAT IS JUDGING YOU
THE IRS WILL *NEVER* ASK YOU TO EMAIL THEM YOUR SSN OR ANY OTHER PERSONAL INFO. DISREGARD THESE FAKE EMAILS THIS TAX SEASON.
YOU CAN REPORT SUSPICIOUS EMAILS TO PHISHING@IRS.GOV
SAC the security awareness COMPANY

Security Quick Tip

Keep your Social Security number private as long as you can and never give it out unless absolutely necessary. Do not carry your Social Security card with you.

For more security tips, news, advisories, and resources visit the Montana Information Security website, find us on Facebook, or follow us on Twitter.

http://sitsd.mt.gov/MontanaInformationSecurity

State of Montana Information Security

@MontanaSecurity

Contact Us:

Enterprise Security Program

Lynne Pizzini, CISO and Deputy Chief Information Officer

Joe Frohlich, Enterprise Security Manager